Exhibit D

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
12/512,873	07/30/2009	Blayn W. Bennau	12655.1600	6515

66170   7590   01/26/2011

Snell & Wilmer L.L.P. (AMEX)
ONE ARIZONA CENTER
400 E. VAN BUREN STREET
PHOENIX, AZ 85004-2202

EXAMINER
REAGAN, JAMES A

ART UNIT	PAPER NUMBER
3621	

NOTIFICATION DATE	DELIVERY MODE
01/26/2011	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

HSOBELMAN@SWLAW.COM
DMIER@SWLAW.COM
JESLICK@SWLAW.COM

PTOL-90A (Rev. 04/07)

Office Action Summary	Application No.	Applicant(s)
	12/512,873	BENNAU ET AL.
	Examiner	Art Unit	
	JAMES A. REAGAN	3621	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 November 2010*.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *30 July 2009* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

U.S. Patent and Trademark Office

PTOL-326 (Rev. 08-06)   **Office Action Summary**   Part of Paper No./Mail Date 20110119

Application/Control Number: 12/512,873   Page 2

Art Unit: 3621

DETAILED ACTION

Status of Claims

1.   This action is in reply to the amendment and response filed on **11/16/2010**.

2.   Claims 1, 4-6, and 8-20 have been amended.

3.   The rejections of claims 1-20 have been updated to reflect the amended limitations. The prior art

of record has not been changed.

4.   Claims 1-20 are currently pending and have been examined.

Application/Control Number: 12/512,873   Page 3

Art Unit: 3621

Response to Arguments

5.   Applicant's arguments received **11/16/2010** have been fully considered but they are not persuasive. Referring to the previous Office action, Examiner has cited relevant portions of the references as a means to illustrate the systems as taught by the prior art. As a means of providing further clarification as to what is taught by the references used in the first Office action, Examiner has expanded the teachings for comprehensibility while maintaining the same grounds of rejection of the claims, except as noted above in the section labeled "Status of Claims." This information is intended to assist in illuminating the teachings of the references while providing evidence that establishes further support for the rejections of the claims.

With regard to the limitations of independent claims 1, 8, and 14, Applicant argues, "…Reno is deficient in at least three ways: (i) Reno is not directed to a browser toolbar (i. e., an e-wallet) that receives personal identifying information. (ii) The toolbar in Reno does not provide an encryption key to a bank server; rather, Reno encrypts a user's login information using a key provided in a digital certificate and before transmitting the information to a bank server. (iii) Reno does not encrypt "personal identifiable information," because a username and password are not information with which a person may be uniquely identified (i.e., they are not akin to a transaction account number and the like).

The examiner respectfully disagrees:

(i)   **RENO**, in at least paragraph 0014 discloses digital signatures and SSL. In addition, **RENO** in at least paragraph 0005 discloses, "The security application may be a tool bar…"

(ii)   There is no mention of a bank server in any of the independent claims as alleged. It appears as if the Applicant is reading limitations into the claims from the specification. Consequently, the points argued are not recited in the claims themselves. For that reason, a solid argument in their contemplation cannot be established. Subsequent amendments to the claim language that would include

Application/Control Number: 12/512,873   Page 4

Art Unit: 3621

the positions presented by the Applicant's arguments would provoke the Examiner to address the claims individually and as a whole, in light of the remaining limitations as well as the specification. Until such amendments are rendered, the arguments are disregarded and will not be countered. In summary, the Examiner has taken the broadest and most reasonable interpretation of the claim limitations as written, in light of the specification. Although the specification may contain recitations of intended use, alternative points of view and subjective interpretative differences between the prior art of record and the present invention as premeditated, it is the claims themselves that are given patentable weight only inasmuch as they are constructed. Because the claimed invention has been painted with the broad stroke of petitioning for limitations that encompasses more than is asserted in the Applicant's claims, the prior art of record continues to fully discloses the Applicant's inventions *as claimed*.

(iii)   There appears to be no definition on the specification regarding what is personally identifiable information. The Examiner has taken the broadest and most reasonable interpretation of the claim limitations as written, in light of the specification. Although the specification may contain recitations of intended use, alternative points of view and subjective interpretative differences between the prior art of record and the present invention as premeditated, it is the claims themselves that are given patentable weight only inasmuch as they are constructed. Because the claimed invention has been painted with the broad stroke of petitioning for limitations that encompasses more than is asserted in the Applicant's claims, the prior art of record continues to fully discloses the Applicant's inventions *as claimed*.

Furthermore, It appears as if the Appellant is attacking the references in a piecewise fashion, instead of in combination, as intended by the Examiner and as shown above in the rejections under 35 USC § 103(a).

Application/Control Number: 12/512,873   Page 5

Art Unit: 3621

6.   With regard to claims 7 and 20, the common knowledge declared to be well-known in the art is

hereby taken to be admitted prior art because the Applicant either failed to traverse the

Examiner's assertion of **OFFICIAL NOTICE** or failed to traverse the Examiner's assertion of

OFFICIAL NOTICE adequately. To adequately traverse the examiner's assertion of **OFFICIAL**

NOTICE, the Applicant must specifically point out the supposed errors in the Examiner's action,

which would include stating why the noticed fact is not considered to be common knowledge or

well-known in the art. A general allegation that the claims define a patentable invention without

any reference to the Examiner's assertion of **OFFICIAL NOTICE** would be inadequate. Support

for the Applicant's assertion of should be included. The Examiner respectfully submits that, in

this case, the Applicant may refer to the background of the specification, page 3, to find evidence

that e-wallet plug-ins are old and well-known in the web-browser arts.

Application/Control Number: 12/512,873   Page 6

Art Unit: 3621

Claim Rejections - 35 USC § 103

7.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness

rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as
set forth in section 102 of this title, if the differences between the subject matter sought to be
patented and the prior art are such that the subject matter as a whole would have been obvious
at the time the invention was made to a person having ordinary skill in the art to which said
subject matter pertains. Patentability shall not be negatived by the manner in which the invention
was made.

8.   The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966),

that are applied for establishing a background for determining obviousness under 35

U.S.C. 103(a) are summarized as follows:

1.   Determining the scope and contents of the prior art.
2.   Ascertaining the differences between the prior art and the claims at issue.
3.   Resolving the level of ordinary skill in the pertinent art.
4.   Considering objective evidence present in the application indicating obviousness or
        nonobviousness.

9.   This application currently names joint inventors. In considering patentability of the claims under

35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was

commonly owned at the time any inventions covered therein were made absent any evidence to

the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor

and invention dates of each claim that was not commonly owned at the time a later invention was

made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35

U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

Application/Control Number: 12/512,873   Page 7

Art Unit: 3621

10.   Claims 1-6, and 8-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Reno et al. (USPGP 2005/0172229 A1), hereinafter **RENO**, in view of Weber (USPGP 2004/0061720 A1), hereinafter **WEBER**.

Claim 1:

RENO as shown below discloses the following limitations:

- *receiving, by a computer-based system for securely downloading customer data to a browser toolbar and via the browser toolbar, via the browser toolbar, a request for customer data from a customer;* (see at least paragraph 0012)

- *determining, by the computer-based system, the request for customer data includes a request for personal identifiable information requiring encryption by a public encryption key generated by the browser toolbar;* (see at least paragraphs 0014, 0022, 0031)

- *authenticating, by the computer-based system, the customer based on a set of a user credential and an account specific access credential,* (see at least paragraph 0013) *wherein:*

  - *the user credential and the account specific access credential are distinct,* (see at least paragraph 0013)

  - *the account specific access credential is associated with an account of the customer;* (see at least paragraph 0013)

- *encrypting, by the computer-based system, the requested personal identifiable information using the public encryption key generated by the browser toolbar;* (see at least paragraph 0035)

RENO does not specifically disclose the limitation of …*requiring encryption by a public encryption key generated by the browser toolbar.* However, **RENO**, in at least paragraph 0014 discloses digital signatures and SSL. In addition, **RENO** in at least paragraph 0005 discloses, "The security application may be a tool bar…" It would have been obvious to one of ordinary skill

Application/Control Number: 12/512,873   Page 8

Art Unit: 3621

in the art at the time of the invention to combine/modify the method of **RENO** with the technique of utilizing PKI from a browser tool bar **because**, "Fraudulent activities on the Internet have increased drastically. Examples include password spoofing, password phishing, and man-in-the-middle attacks. "Spoofing" and "phishing" generally refer to the practice by nefarious parties of fooling a web user into providing sensitive information, such as passwords, personal information, financial information, and the like, by imitating a web site the user trusts. "Man-in-the-middle attack" (MITM) generally refers to the practice of sniffing packets from a network, possibly modifying them, then returning them to the network. MITM typically requires comprising a sender's and/or a receiver's public key. In part, these fraudulent activities are successful because users are trained to enter sensitive information directly into web forms and popup windows. The content and appearance of these windows are easy to spoof since they are based on ordinary HTML. Any content delivered over the web, however, is easy to duplicate for the purposes of setting up a fake web site. In general there is risk whenever one wants to share sensitive information via a network. Thus, systems and methods are needed that assist users to not provide sensitive information to untrusted entities." (**RENO**: paragraph 0003)

RENO does not disclose the limitation of *transmitting the encrypted personal identifiable information to the browser toolbar*. However, **WEBER**, in at least paragraphs 0008, 0019, and 0023 discloses transmission of data from the browser toolbar. It would have been obvious to one of ordinary skill in the art at the time of the invention to combine/modify the method of **RENO** with the technique of **WEBER** because, "Fraudulent activities on the Internet have increased drastically. Examples include password spoofing, password phishing, and man-in-the-middle attacks. "Spoofing" and "phishing" generally refer to the practice by nefarious parties of fooling a web user into providing sensitive information, such as passwords, personal information, financial information, and the like, by imitating a web site the user trusts. "Man-in-the-middle attack" (MITM) generally refers to the practice of sniffing packets from a network, possibly modifying them, then returning them to the network. MITM typically requires comprising a sender's and/or a receiver's public key. In part, these fraudulent activities are successful because users are trained

Application/Control Number: 12/512,873   Page 9

Art Unit: 3621

to enter sensitive information directly into web forms and popup windows. The content and

appearance of these windows are easy to spoof since they are based on ordinary HTML. Any

content delivered over the web, however, is easy to duplicate for the purposes of setting up a

fake web site. In general there is risk whenever one wants to share sensitive information via a

network. Thus, systems and methods are needed that assist users to not provide sensitive

information to untrusted entities." (**RENO**: paragraph 0003)

Claim 2:

The combination of **RENO/WEBER** discloses the limitations as shown in the rejections

above. **RENO** further discloses *creating a public/private key pair combination in response to the*

detecting (see at least paragraph 0035).   **RENO** does not specifically disclose the following

limitations, but **WEBER** as shown does:

- *analyzing, by the browser toolbar, web services initiated on a computer system*
  executing the browser toolbar; (see at least paragraph 0004)

- *detecting, based at least in part on the analyzing, when the request for customer*
  data includes the request for personal identifiable information; (see at least
  paragraph 0006)

It would have been obvious to one of ordinary skill in the art at the time of the invention to

combine/modify the method of **RENO** with the technique of **WEBER** because, "Fraudulent

activities on the Internet have increased drastically. Examples include password spoofing,

password phishing, and man-in-the-middle attacks. "Spoofing" and "phishing" generally refer to

the practice by nefarious parties of fooling a web user into providing sensitive information, such

as passwords, personal information, financial information, and the like, by imitating a web site the

user trusts. "Man-in-the-middle attack" (MITM) generally refers to the practice of sniffing packets

from a network, possibly modifying them, then returning them to the network. MITM typically

requires comprising a sender's and/or a receiver's public key. In part, these fraudulent activities

are successful because users are trained to enter sensitive information directly into web forms

Application/Control Number: 12/512,873   Page 10

Art Unit: 3621

and popup windows. The content and appearance of these windows are easy to spoof since they

are based on ordinary HTML. Any content delivered over the web, however, is easy to duplicate

for the purposes of setting up a fake web site. In general there is risk whenever one wants to

share sensitive information via a network. Thus, systems and methods are needed that assist

users to not provide sensitive information to untrusted entities." (**RENO**: paragraph 0003)

Claim 3:

The combination of **RENO/WEBER** discloses the limitations as shown in the rejections

above. **RENO** further discloses *the account specific access credential includes a card security*

code associated with the customer. See at least paragraph 0034.

Claims 4-6:

The combination of **RENO/WEBER** discloses the limitations as shown in the rejections

above. **RENO** further discloses:

- *determining, by the computer-based system, that the account of the customer is*

   eligible for use with a web service initiating the request for customer data; (see at

   least paragraph 0029)

- *retrieving, by the computer-based system, generic account data associated with*

   the account, wherein the generic account data includes information for the

   customer to decipher the account from another; (see at least paragraph 0034)

- *transmitting, by the computer-based system, the generic account data to a*

   computer system executing the browser toolbar. (see at least paragraph 0012)

- *the generic account data includes a portion of an account number associated*

   with the account of the customer. (see at least paragraph 0034)

- *receiving, via a user interface, a selection request indicating the customer*

   requests access to personal identifiable information associated with the account

   of the customer; (see at least paragraphs 0012-0015)

Application/Control Number: 12/512,873   Page 11

Art Unit: 3621

- *determining whether the customer has access to the personal identifiable information associated with the account of the customer based at least in part on the account specific access credential.* (see at least paragraphs 0012-0015)

Claims 8-19:

The combination of **RENO**/**WEBER** discloses the limitations as shown in the rejections of the claims above. The Examiner finds that remaining claims 8-19 are not patentably distinct from claims 1-6, nor do they produce any new, meaningful, synergetic result that would render the claims novel and therefore, for the sake of clarity, has grouped the rejections of claims 1-6 and 8-19 accordingly using the same references and citations as above.

Application/Control Number: 12/512,873   Page 12

Art Unit: 3621

11.   Claims 7 and 20 rejected under 35 U.S.C. 103(a) as being unpatentable over **RENO/WEBER** and

further in view of Examiner's **OFFICIAL NOTICE**.

Claims 7 and 20:

The combination of **RENO/WEBER** discloses the browser toolbar application as shown in

the rejections above.   **RENO/WEBER** does not specifically state *the encrypted personal*

identifiable information is decrypted by the browser toolbar and stored in an e-wallet.   However,

the Examiner takes **OFFICIAL NOTICE** that it is old and well known in the online transaction and

e-commerce arts to utilize electronic purses and wallets.   It would have been obvious to one of

ordinary skill in the art at the time of the invention to combine/modify the method of

RENO/WEBER with the technique of an e-wallet because "Fraudulent activities on the Internet

have increased drastically. Examples include password spoofing, password phishing, and man-

in-the-middle attacks.   "Spoofing" and "phishing" generally refer to the practice by nefarious

parties of fooling a web user into providing sensitive information, such as passwords, personal

information, financial information, and the like, by imitating a web site the user trusts.   "Man-in-

the-middle attack" (MITM) generally refers to the practice of sniffing packets from a network,

possibly modifying them, then returning them to the network. MITM typically requires comprising

a sender's and/or a receiver's public key.   In part, these fraudulent activities are successful

because users are trained to enter sensitive information directly into web forms and popup

windows. The content and appearance of these windows are easy to spoof since they are based

on ordinary HTML.   Any content delivered over the web, however, is easy to duplicate for the

purposes of setting up a fake web site.   In general there is risk whenever one wants to share

sensitive information via a network. Thus, systems and methods are needed that assist users to

not provide sensitive information to untrusted entities." (**RENO**: paragraph 0003).

Application/Control Number: 12/512,873   Page 13

Art Unit: 3621

CONCLUSION

12.   Applicant's amendment filed on **11/16/2010** necessitated the new ground(s) of rejection presented in this Office action. Accordingly, THIS ACTION IS MADE FINAL. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

13.   A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

14.   Any inquiry of a general nature or relating to the status of this application or concerning this communication or earlier communications from the Examiner should be directed to **James A. Reagan** (james.reagan@uspto.gov) whose telephone number is **571.272.6710.** The Examiner can normally be reached on Monday-Friday, 9:30am-5:00pm. If attempts to reach the examiner by telephone are unsuccessful, the Examiner's supervisor, **ANDREW J. FISCHER** can be reached at **571.272.6779**.

15.   Should Applicant desire in the future to receive formal or informal email communications from the Examiner (e.g. acknowledgments, references, courtesy copies of documents, etc.), the electronic file must contain written authorization to conduct email communications. See MPEP §502.03 III. For Applicant's benefit, exemplary language for written authorization is in MPEP §502.03 III. ¶4. The exemplary language is:

Application/Control Number: 12/512,873   Page 14

Art Unit: 3621

> ***Recognizing that Internet communications are not secure, I hereby authorize the USPTO to communicate with me concerning any subject matter of this application by electronic mail. I understand that a copy of these communications will be made of record in the application file.***

16.   In the situation where Applicant desires to receive email communications from the Examiner, the Examiner suggests placing the above exemplary language in Applicant's next correspondence.

17.   Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system.   Status information for published applications may be obtained from either Private PAIR or Public PAIR.   Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://portal.uspto.gov/external/portal/pair . Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at **866.217.9197** (toll-free).

18.   Any response to this action should be mailed to:

<div align="center">

Commissioner of Patents and Trademarks

Washington, D.C. 20231

</div>

        or faxed to **571-273-8300**.

19.   Hand delivered responses should be brought to the **United States Patent and Trademark Office Customer Service Window**:

<div align="center">

Randolph Building

401 Dulany Street

Alexandria, VA 22314.

</div>

/James A. Reagan/
Primary Examiner, Art Unit 3621
james.reagan@uspto.gov
571.272.6710 (Office)
571.273.6710 (Desktop Fax)